Y2K Cookbook

Year 2000 Guide for California's Local Governments

A Partnership between the
Department of Information Technology
and Merced County, California

Special Edition:
Prepared by the State of California,
Department of Information Technology
September, 1999

Includes information about tools and resources available from the State of California

State of California
Department of Information Technology
801 K Street
Sacramento, CA 95814
916-445-5900
www.year2000.ca.gov

Merced County
2222 M Street
Merced, CA 95340
209-385-7434
www.co.merced.ca.us

TABLE OF CONTENTS

Y2K Cookbook

INTRODUCTION

This ***Y2K Cookbook*** is the result of a partnership project between the State of California Department of Information Technology and Merced County, California. Under direction of Governor Gray Davis, a State Year 2000 and Information Technology transition team examined multiple layers of Y2K issues. One conclusion identified was the need for the State of California and its local counties to cooperate together to minimize Y2K-related disruptions. The team proposed a pilot project where the State would collaborate with a county to review and evaluate the county's Y2K remediation efforts. To this end, the Department of Information Technology and Merced County joined together to develop a prototype assessment program, which could be used by other local governments to enhance preparedness for the Year 2000.

This project was a valuable opportunity for the purpose of helping to ensure that California – its citizens and businesses – are afforded the smoothest possible transition to the Year 2000, and that they are not adversely impacted by any failure on the part of California's governments to effectively deal with the Year 2000 problem.

It is our hope that local governments facing the Y2K challenge will be well equipped and prepared to usher in the new millennium.

Merced County Board of Supervisors
Gloria Cortez Keene, District 1
Kathleen M. Crookham, District 2
Joe Rivero, District 3
Deidre F. Kelsey, District 4
Jerry O'Banion, District 5

Gregory B. Wellman
County Administrative Officer

OVERVIEW

Year 2000 is fast approaching and it is imperative that California's state and local governments are prepared to continue critical business functions with few, if any, disruptions due to the changeover at the end of the year. With the increased dependence on technology, state governmental entities regularly work in concert with local government organizations to deliver services to the public. The result of this interdependency is that if the computer system of one governmental entity is disrupted, it could affect the automated operations of other governmental entities. Therefore, it is essential that local government be successful in Year 2000 remediation efforts because of the vital role local government plays in the delivery of essential services to the state's 33 million citizens.

This ***Y2K Cookbook*** shares the lessons learned from the partnership project between the State of California and Merced County. It will outline the same steps taken to complete a preparedness evaluation for Merced County. Other local governments must realize that this Guide is not an all-inclusive handbook; rather it is a tool intended to share with others what was learned and gleaned from the experience. Merced County claims no expressed or implied warranty for the methods contained herein. Therefore, use this as a Guide for Y2K efforts, acknowledging that each entity is unique to itself, with its own challenges and vulnerabilities.

INVENTORY

LIST EVERYTHING

The first thing that any organization should do is to create a list of automated systems that might be affected by the Year 2000 problem. Enlist the help of everyone in the organization to identify all systems that contain program logic.

The following is a sampling of items to consider:

> ⌘ ***Think broad! Y2K is more than just a computer-related problem. It can affect <u>any</u> automated system.***

- Public Works Hardware
- Flow Control Devices
- Global Positioning Systems
- Elevators
- Power Plants
- Security Systems (Doors, Locks, etc.)
- Water Treatment, Potable
- Waste Water Treatment
- Plumbing Systems

- Transportation Systems
- Freeway Metering Systems
- Highway Transportation Controls
- Mass Transit Systems
- Rail Automated Switching Systems
- Traffic Light Controllers
- General Services Systems
- Electrical Distribution Systems
- Electric Appliances
- Electric Utility Substations
- Heating or Cooling Systems
- Lighting Controls
- Emergency Shutdown Systems
- Communications Infrastructure
- Microwave Communications Systems
- Telephone Switches (Pagers, Cell Phones, Telephones, Phone Cards)

LIST EVERYTHING - Continued

- Management/Maintenance Systems
- Other Mainframe Applications
- Payroll Systems
- Billing Systems
- Permit Applications Systems
- Police CAD Systems
- Procurement Applications
- Wanted Vehicle Systems
- Revenue Systems
- Street/Location Systems
- Loan/Mortgage Systems
- Public Records Indexing Systems
- Utility Billing Applications
- Wanted Persons Systems
- Hand-held Software (Parking Tickets, Meter Reading, etc.)
- Data
- Mainframe Databases
- Network Server Databases
- Personal Computer Databases
- Computers
- Desktop Computers
- Mainframes
- Software on Mainframes
- Network Computers
- Mobile Data Terminals
- Hand-held Computing Devices
- Software on Networks or Desktops
- Electronic Spreadsheets

- (Ad Valorum) Tax Systems
- Criminal Records Systems
- Criminal Justice Systems
- Drivers Licensing Networks
- Financial Management Systems
- Finger Print Identification Systems
- Fire CAD Systems
- Human Resource Systems
- Identification Systems
- Inventory Control Systems
- Alarm Systems (Clocks)
- Cash Registers
- Pocket Organizers
- Travel Services
- Office Equipment (Photocopiers, Fax Machines, Post Scales, Video Equipment)
- Banking Hardware (ATM Machines, Credit Cards)
- Banking Services (Funds Transfer, Clearing Services)
- Citizen Services (Library Cards)
- Hospital Equipment
- Health Records Databases
- Air Traffic Controls
- Vehicle Automated Systems

GATHER INFORMATION

When all of the potentially affected systems have been identified, collect information on each system. The information will assist in prioritizing the most critical systems for an organization. Most organizations will not finish remediation on all of their systems. Therefore, every organization must carefully prioritize its applications, putting what is most critical to its self-preservation first. Collecting basic information from the users, developers and vendors of each system will ensure that the task of prioritization is an educated decision.

It is essential that the information collected is complete, clear and accurate. The depth and breadth of time spent on gathering data can be as long or as short as needed. The quicker course includes obtaining very basic data such as the following:

- Name and Description
- Location
- Date Dependency
- Embedded Processor Included
- Number of Users
- Contact Person

A more detailed profile of the system would add:

- Developer/Vendor
- Primary Functions
- System Interfaces
- Volume and Rate of Transactions
- Software Platform, Operating Systems, Language, Size
- Analysis Method
- Remediation Methods and Status

Refer to Form A – Department Inventory and Form B – Critical System Evaluation in the Appendix for examples of forms used to gather information.

SOFTWARE SYSTEMS

There are basically two types of software: commercial-off-the-shelf software and custom developed software.

For commercial-off-the-shelf software, an organization will obtain information from the software manufacturer. Most companies have Internet websites publishing whether their applications are Y2K compliant. An organization will want to obtain a letter or certificate of Y2K compliance or specific plans for becoming compliant. Additional measures that add depth to the evaluation include the fixing logic, test methods and reports. If a software program will not be compliant, be sure to obtain from the manufacturer suggested workarounds.

Refer to Form C – Y2K Certification Request in the Appendix for sample letter of request.

Custom developed software refers to the “home-grown” application programmed for specific purposes or departments within an organization. Many local governments have information technology departments, which write mainframe applications. Evaluation of custom software systems will enable the organization to determine how much of the system is complete and Y2K compliant.

EMBEDDED SYSTEMS

Local governments will be surprised to know that there are more embedded systems at large in the organization than estimated. Essential business components depend on the operation of microelectronic circuits known as "embedded systems".

Like commercial software manufacturers, most companies have Internet websites publishing whether their equipment (wherein the embedded system may be located) is Y2K compliant. An organization will want to obtain a letter or certificate of Y2K compliance or specific plans for becoming compliant. Additional measures that add depth to the evaluation include the fixing logic, test methods and reports. If a specific embedded system will not be compliant, be sure to obtain from the manufacturer contingency suggestions.

Additional Tools

The State of California created a guide for developing solutions to embedded systems problems. Although written for the State of California, this methodology can serve as a guide for other organizations seeking to address the embedded systems issue.

California Year 2000 Embedded Systems Program Guide *- This document describes the framework for developing and implementing solutions to embedded microchip problems in automated devices. Although written for the State of California, it includes a methodology that organizations can use as a guide to ensure the proper functioning of their embedded systems into the next millennium. The following documents supplement the program guide:*

Sample Year 2000 Testing Conditions (Scenarios)
Year 2000 Consultant Services Model Statements of Work
Y2K Continuity Planning for Business
Y2K Embedded Systems
Y2K External Interfaces
Y2k Telecommunications
Y2K Voice Recognition

To access these documents, please visit the State of California's Year 2000 web site at:

www.year2000.ca.gov/publications

(Information provided by the State of California, Department of Information Technology)

There are also specialty firms, which address embedded system issues. These firms inventory all known embedded systems in buildings and vehicles. They evaluate and provide an assessment as well as recommendations of actions for remediation.

INTERFACES

It is hard to imagine any organization as a separate entity. In today's world, many local governments are realizing that interdependencies are rampant. Many local governments may use state or federal systems, or be linked with school systems, or partner with business services. These interface relationships must be included in the evaluation of an organization's systems. Although each entity may pursue separate Y2K efforts, collaboration is essential for successful Y2K compliance.

⌘ ***Who do you interface with?***

Evaluating interfaces demands that organizations network, communicate and share information. Identify external relationships and interfaces when gathering data. Interfaces may include:

- Federal Government
- State Government
- Counties
- Cities and Municipalities
- Special Districts and Agencies
- Businesses
- Community Organizations
- Schools
- Citizens

RISK ASSESSMENT

Once the inventory is complete, the organization should assess the risk involved with each system. The assessment includes measuring the progress of the remediation activities for different types of systems.

YEAR 2000 PREPAREDNESS

Each organization needs to determine critical deadlines or completion dates to measure the readiness of the various systems. When identifying key dates, ensure that adequate time is allotted for testing. It isn't enough to merely finish programming before December 31, 1999. It is equally important to have thorough tests concluded well before the rollover.

⌘ ***Will the system be ready by your critical dates?***

BUSINESS CONTINUITY PLANS

It is recommended that an organization take all necessary steps to ensure the continuous delivery of essential services. Include in the organization's assessment a review of contingency plans. Contingency planning involves designing "What if?" scenarios with multi-layered alternatives, including manual processes. For each system, especially those identified as most critical, the organization should have pre-planned response activities to react to failure scenarios. Depending on the criticality of the system, it may be necessary to have more than one backup plan in place.

There are various methods for providing business continuity. An organization will discover that some systems, such as a power generator, are backups for others. Having a manual process or procedure or other systems or individuals who perform the same process are other options, while some systems may not have a continuity strategy.

Additional Tools

The State of California has a methodology for developing business continuity plans along with a variety of tools that can be used with the methodology. Although written for the State of California, this methodology can serve as a guide for other organizations seeking to develop business continuity plans.

Continuity Planning for Business Methodology (CPB) Documents *– The CPB methodology consists of three components: a Reference Guide, Workbook and Toolkit. The Reference Guide provides an in-depth discussion on the CPB process. The Workbook is an intuitive tool designed to guide an organization through the entire life cycle of the planning process. The Toolkit includes the tools referenced in the Guide and Workbook. For example, it includes a timeline to help structure the planning effort, worksheets to assist in mapping processes and resources, a template to assist in documenting the actual continuity plan, and a glossary of CPB terms.*

CPB Workbook
CPB Reference Guide
CPB Toolkit

Continuity Planning for Business (CPB) Toolkit *- The CPB program is a comprehensive program designed to assist organizations in the development of CPB plans to ensure the continuity of mission-critical services.*

Initial CPB Reporting Documents
Baseline Questionnaire
CPB Initial Report Instructions
CPB Rollout Memo Package
Definition of Mission-Critical

To access these documents, please visit the State of California's Year 2000 web site at:

www.year2000.ca.gov/publications

(Information provided by the State of California, Department of Information Technology)

UNAVAILABILITY IMPACT

When conducting a risk assessment, ensure that impacts caused by unavailability of systems due to Year 2000 problems are identified and assessed. While few applications would actually impact public safety or property loss, many could cause varying levels of hardship on employees or clients. The organization must always consider the consequences of not being able to use a specific item.

⌘ What would happen if the system were not available for use?

Losing the function for receiving 911 emergency calls or dispatching emergency vehicles (either police or fire) could create a critical situation where public safety is in jeopardy or public property is at risk. Or the loss of power could make most traffic signals and railroad crossing controls inoperative, potentially causing personal injury or property loss.

Other systems, which could cause varying degrees of hardship, revolve around the organization's ability to meet its day-to-day obligations. These include:

- Wide or Local Area Networks (Personal Computers and Application Software)
- Mainframe Computer Systems (Peripheral Equipment and Application Software
- Public Assistance Benefit Delivery and Reporting (Cash and Food Stamp)
- Payroll (for General Staff, Retirees and General Service Providers)
- Probation Case Management
- Juvenile Hall Operation
- Financial Management Systems (Accounts Payable, General Ledger, Cost, etc.)
- Telephone Systems
- Public Facilities Management and Control (HVAC, Elevators, Alarms)
- Correctional facilities (Alarms, Automatic Controls, Lighting, Booking and Release Information)
- Mental Health and Public Health Case Management Tools
- Jury System
- Court Calendaring
- Criminal Warrant Processing
- Family Support Collections and Disbursements
- Revenue Collections (Utilities, Taxes, etc.)

DOWN TIME TOLERANCE

Another indicator of the risk involved with a particular system is predicting the down time tolerance. Any organization should ask itself how long could a system be down until it causes a significant impact. For instance, an email system could be down for 10 days with little impact; however, the failure of the correctional facility automated cell locking system will have instant impact. The automated cell locking system cannot tolerate any down time to occur.

⌘ ***How long can you manage, if the system was not available?***

Systems that have a low volume in use can be allowed to be down and inoperable for longer periods of time. Organizations may find that there is no tolerance level for certain systems, such as backup generators systems. The level of tolerance for down time will vary between organizations as well as between departments and even users within the organization.

PRIORITZE

Prioritization is defining the focus of Y2K efforts for an organization. Based on the information gathered in the inventory, key organization staff will determine what systems demand immediate attention. An organization must identify and prioritize functions that must be made Y2K compliant immediately and those other functions, which can be addressed later. Prioritization will focus energies on what will have the most impact.

⌘ ***What matters most to your organization?***

For a local government, there are many things to consider, and each organization needs to develop its own strategy for determining priorities. Some basic categorical impacts to consider in terms of prioritization include:

- Public Safety – threatens the public (alarm/security systems, correctional facility locking systems)
- Life Threatening – poses immediate danger (911 emergency services, life support systems)
- Officer Safety – threatens peace officers (criminal databases)
- Health and Welfare Services – impacts citizens (welfare check printing systems)
- Financial Stability – threatens revenue streams (tax and billing systems)
- Legal Implications – compromises legal requirements (court systems)
- Public Services – decreases services to citizens (library cards, recreational facilities)

Other information to consider comes from the risk assessment of the each system. Systems that have backup sources, contingency plans, manufacturer certification, testing validation are better prepared than others. When completing the task of prioritization, always ask what kinds of impacts would unavailability non-compliance have on the members of the organization.

Local governments are in a precarious position, as a provider of services to thousands of citizens. The impact of Y2K will not only affect members of the local government organization, but all citizens within as well as outside of its boundaries. Thus prioritization is essential to the Y2K efforts of an organization.

REMEDIATION AND MITIGATION

While an organization may hope to have every possible issue fixed, many will have to settle on a combination of remediation and mitigation efforts.

Remediation is choosing to fix the problem. There are generally five technical solutions to the Year 2000 problem:

- Conversion – change every date to a four-digit year
- Fixed windowing – create a 100-year window such as 1929 and 2029 and if the two digit year is greater than 29, then the program assumes the century digits to be 19; if the two-year digit is less than or equal to 29, the century digits are assumed to be 20
- Sliding windowing – similar to fixed windowing except the 100-year window is calculated from the current date
- Encryption –compress dates with four-digit years to occupy the same storage space as dates with two-digit years
- Encapsulation – reset the year to 28 years earlier, useful only in embedded process controllers in which the year is not important but the day of the week is important

Remediation can be demanding and time consuming, especially for an organization that relies on customized application software. There may be millions of lines of program code to change, as well as invalid date comparisons.

Opting to mitigate a problem means that the organization will create a plan that works around the problem. It could be replacing a system with a newer Y2K compliant version or reverting to a manual process. It may also require simply dealing with a usable but non-compliant non-critical system until a later date when it can be remediated.

Refer to Form D – Sample Mitigation Plans in the Appendix mitigation suggestions.

PUBLIC AWARENESS

SHARE INFORMATION

All organizations, especially local governments, should include in their Y2K efforts public awareness. The more informed people are, the less fearful they behave. There is so much information in the news about the Year 2000 problem ranging from the switch marking the end of the world or the optimistic opinion that Y2K will not cause a single problem. Individuals should realize that the reality will lie somewhere between those two extremes.

Organizations are encouraged to share their work and progress with its internal associates as well as its external customers and constituents. Honest communications will inform the public of what services are guaranteed available, precautionary measures to take and business continuity plans that will be in place. Local elected officials are encouraged to partners with business and community leaders to collaborate. Ideas for raising public awareness include:

- Community forums
- Regular media publications
- Business roundtables
- Outreach programs
- Public service announcements

Additional Tools

The State of California has a variety of tools that can be used in the development and implementation of communications and outreach activities. Although written for the State of California, these tools can serve as a guide for other organizations seeking to conduct communication and outreach activities.

Key Messages – *This document outlines the State's primary key messages regarding Y2K. These messages can be used by other organizations as a starting point for developing their own Y2K messages or they can be incorporated into the organization's existing communication and outreach activities*.

Public Information Officers (PIOs) Toolkit - *These documents can assist public information officers in the development, implementation, and tracking of communication and outreach strategies and action plans. The PIO Toolkit includes:*

Communicating with Employees, the Public and the Media about Y2K
Entity Communication and Outreach Strategy Template
Communications Media/Legislative Log Sheet
California's PIO Process Chart

Event Planning Toolkit *- This generic toolkit provides templates for planning and preparing for an outreach event. It includes templates for invitations, letters, minutes, and evaluations, as well as sample name badges and signs and a planning checklist.*

Roundtable Toolkit *– This toolkit provides a guide and template on how to prepare for a Roundtable. The State has used Roundtables as a forum for bringing together service providers in a given industry such as transportation, water, telecommunications, and power, to discuss the industry's Y2K readiness status and to identify industry-specific Y2K concerns. The toolkit includes templates and sample documents similar to those in the Event Toolkit; however, the roundtable templates are more detailed and specifically tailored to the roundtable format.*

To access these documents, please visit the State of California's Year 2000 web site at:

www.year2000.ca.gov/publications

(Information provided by the State of California, Department of Information Technology)

CONCLUSIONS

The Year 2000 is a real problem and organizational preparation is essential to ensure that the citizens of the State of California are not adversely impacted. The majority of potential Year 2000 problems discovered within local governments can be identified and anticipated using the following steps:

- Start today.
- Inventory everything.
- Acknowledge and assess the organization's vulnerabilities.
- Focus on what is most critical to your organization and tend to those items first.
- Have a plan in place to ensure that business continues as best as possible.
- Share your progress and status both internally and externally to increase awareness and reduce fears.

APPENDIX

- Form A Department Inventory
- Form B Critical System Evaluation
- Form C Y2K Certification Request
- Form D Sample Mitigation Plans

DEPARTMENT INVENTORY

Department Information:

Department Name: _____

Department Head: _____

Contact Person: _____ Position: _____

Location/Address: _____ Phone: _____

Email: _____ Fax: _____

Systems Information:

CRITICAL END SYSTEMS

Identify only those systems that are MOST critical to the department's process control and operation, including stand-alone PCs, spreadsheets, databases, etc. (*CRITICAL* meaning the inoperation of the system presents potential harm or loss of life, property or revenue.)

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

INTERMEDIATE SYSTEMS

List all other systems used in the department that are not of a critical nature. Include systems and applications developed internally (by Data Processing or by department members) and applications developed by external third party sources (consultant firms, etc.).

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

(Continued on back)

BUSINESS SUPPORT SYSTEMS
Identify non-information systems and equipment subject to potential impact (i.e. elevators, badge readers, pagers, building environmental control systems, etc.).

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Description: _____

Form Completed By: _____ *Date:* _____

CRITICAL SYSTEM EVALUATION

1. ***Critical System ID***:
2. ***Critical System Name***:
3. ***Task Assignee***:
4. ***Owner***:
5. ***Supplier/Vendor***:
6. ***System Contacts***:

Name	Organization	Responsibility	Telephone

7. System Description

7.1. Brief Description

7.2. Primary Functions

a.

b.

c.

7.3. System Type

[ ] Software System

[ ] Embedded Processor System

[ ] Non-Processor System

7.4. System Interfaces

Interface	Input	Output

7.5. System Operations

a. **Does System Use Dates? [ ] Yes [ ] No**

If Yes, describe how system uses dates:

b. **Volume and Rate of System Transactions**

[ ] High [ ] Medium [ ] Low

Details:

c. **Critical Monthly Events**

8. Non-Compliant Y2K Impacts

[ ] High [ ] Medium [ ] Low

Details:

9. System Unavailability Impacts (Emergency Conditions)

[ ] High [ ] Medium [ ] Low

Details:

10. Software Systems

10.1. Platform

[ ] Mainframe [ ] Workstation [ ] Server [ ] Other:

10.2. Operating System

[ ] DOS [ ] Windows 95/98 [ ] Windows NT [ ] Unix [ ] CMS/VSE [ ] VSE/VM

[ ] Other:

10.3. Language

[ ] COBOL [ ] NATURAL [ ] C, C+, C++ [ ] Visual Basic [ ] Other:

10.4. Software Size

a. **Number of Programs/Modules**:

b. **Source Lines of Code (SLOCS):**

c. **Other Measures of Size:**

10.5. Y2K Analysis

a. **Analysis Method**

Line-By-Line:

Tools:

Other:

b. **Remediation Methods**

Fixed Window/Year:

Sliding Window/Year:

Other:

10.6. Remediation Status

Program/Module	Percent Complete			
	Analysis	Updates	Unit Tests	System Tests

Program/Module	Actual/Plan Date Complete			
	Analysis	Updates	Unit Tests	System Tests

10.7. Is System Operational? [ ] Yes [ ] No

11. Embedded Processor and Vendor Supplied Systems

11.1. Certification of Y2K Compliance:

11.2. Plans for Y2K Compliance:

11.3. Test Reports for Y2K Compliance:

11.4. Status of Y2K Compliance

a. **Percent Complete:**

b. **Actual/Plan Date Complete:**

12. Risk Analysis

12.1. Risk Assessment

a. **Any Risks? [ ] Yes [ ] No**

b. **If Yes, Identify Risks:**

c. **Degree of Risk: [ ] High [ ] Medium [ ] Low**

d. **Probability of Risk Occurring: [ ] High [ ] Medium [ ] Low**

12.2. Risk Mitigation

a. **Method and Plan**

b. **Expected Results**

13. Comments

14. Recommendations

Y2K CERTIFICATION REQUEST

Date

XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX

Dear Sir/Madam:

Like most businesses, ***[Name of organization]*** continues to address the Year 200 issue. We are requesting industry vendors, contractors, and suppliers inform us on the compliance issues of their proprietary systems, hardware, firmware, and applications, as well as embedded chip technologies in equipment supplied to our organization.

We are requesting a letter of certification indicating whether the products and/or services that you manufactured, supplied or maintain are Year 2000 compliant. Our definition of Year 2000 compliant means the equipment will handle the date correctly now, at the turn of the century (Year 2000) and beyond (including leap years) and that date sensitivity is not an issue.

If this equipment, product or service is not Year 2000 compliant, what steps are you taking to ensure that it becomes Year 2000 compliant? Further, what specific dates will the equipment, product or service be Year 2000 compliant and how will your organization validate compliance?

Thank you for your immediate attention and written response to this matter. We look forward to your immediate written response to this matter at your first opportunity but within 30 days of receipt of this letter. If you have any questions or concerns related to this request, please contact, [Name] at [Phone]. Please mail all your correspondence to:

XXXXXXXXXX
XXXXXXXXXX
XXXXXXXXXX

Sincerely,

XXXXXXXXXX

SAMPLE MITIGATION PLANS

COMMUNICATONS

SYSTEM	MITIGATION
Enhanced 911 system	Plan for degraded communication using other available systems.
Radio communications	Use backup power, if available. Plan to use alternate communication systems. Multiple units mean that the loss of one is not a major problem.
Telephone	Provide battery powered radio communication at every facility and for cellular phones. Instruct all personnel in its use and locations.

GENERAL SERVICES

SYSTEM	MITIGATION
Bank reconciliation systems	Continue to collect data from the bank with workstations running on backup power. Check with banks for their plans to retain data longer than two days if they experience Y2K problems.
Central accounting systems	Issue manual receipts. Manually process deposits. Provide personnel to process backlog.
Cost accounting systems	Consider manual processing. Prepare to work off backlog with additional resources.
General ledger systems	Ensure that system is Y2K compliant before June 30, 1999. Provide workstations running on backup power. Could manage up to a week manually, then significant backlog would result because of the high volume of transactions. Provide workstations running on backup power.
Payroll and personnel systems	Determine first pay date for 2000. Consider preprinting checks before the transition is being considered. Provide workstations running on backup power.
Billing systems	Produce hardcopy list of customers late in December to facilitate manual operation. Obtain additional personnel to enter backlog of data.

INFRASTRUCTURE

SYSTEM	MITIGATION
Backup generators	Plan for degradation of communications using devices that are independent of station power source. Provide adequate stand-alone fuel supply. Properly test ability of generators to provide backup power.
HVAC, heating and air conditioning systems	Use manual override or backup power, if available.
Public utilities	Install backup generators. Perform work manually, where feasible.
Traffic signals	Manual traffic control, if personnel available. Back up power source.

COURT OPERATONS

SYSTEM	MITIGATION
CLETS	Use backup power in event of a power failure.
Criminal case and court calendaring systems	Produce January 2000 calendars in late December. Revert to manual record keeping and processing. Ensure that adequate personnel are available to process manually and to handle any data entry backlog.
Jury systems	Prepare and print out January and February jury calls early.
Jail door controls	Operate manually using keys.

OTHER SYSTEMS

SYSTEM	MITIGATION
Lab testing system	Plan process and prepare hardcopy to facilitate degraded manual processing. Obtain additional personnel to enter backlog of data.
Welfare services systems	Use limited manual processing where possible. Backup power supplies. Provide additional personnel to process manually and to work down backlog when system available.
Permit tracking system	Issue permits and schedule inspections manually. Collect data for later entry. Use backup power supply.